JOURNAL OF COMBINATORIAL THEORY, Series A 42, 296–299 (1986)

Note

Reconstructing the Ternary Golay Code

DONALD Y. GOLDBERG

Occidental College, Los Angeles, California 90041

Communicated by the Managing Editors

Received June 11, 1985

The Golay codes, first constructed by Golay in 1949 ([3], see [6]), have since been extensively studied by coding theorists [6, especially Chaps. 2, 16, 20], sphere packers [5], constructors of simple groups [2], and design theorists [1].

Wolfmann [8] described the [24, 12, 8] extended binary Golay code as "the binary image, relative to a certain basis, of a principal ideal" in a group algebra over the field of 8 elements. We present an analogous description of the [12, 6, 6] extended ternary Golay code as the image of a code over the field of 9 elements. We also describe the weight structure of the pre-image code.

An $[n, k, d]$ linear code $\mathscr{C}$ over the finite field F is a k-dimensional subspace of F^n for which $d = \min\{wt(\mathbf{v}): \mathbf{v} \in \mathscr{C}, \mathbf{v} \neq 0\}$, where $wt(\mathbf{v})$ denotes the Hamming weight of $\mathbf{v}$, the number of nonzero components in $\mathbf{v}$. Two codes are equivalent if an F-monomial transformation maps one code onto the other.

The extended ternary Golay code $\mathscr{G}_{12}$ may be defined as the row space in $GF(3)$ of the matrix

$$\begin{bmatrix} 1 & & & & & 0 & 1 & 1 & 1 & 1 & 1 \\ & 1 & & & & 1 & 0 & 1 & -1 & -1 & 1 \\ & & 1 & & & 1 & 1 & 0 & 1 & -1 & -1 \\ & & & 1 & & 1 & -1 & 1 & 0 & 1 & -1 \\ & & & & 1 & 1 & -1 & -1 & 1 & 0 & 1 \\ & & & & & 1 & 1 & -1 & -1 & 1 & 0 \end{bmatrix};$$

other definitions are available [6]. Pless has characterized the extended ternary Golay code among linear codes.

0097-3165/86 $3.00

THEOREM (Pless [7]). *Any* $[12, 6, 6]$ *code over* $GF(3)$ *is equivalent to* $\mathscr{G}_{12}$.

Let $F = GF(3) = \{0, 1, 2\}$ and $K = GF(9) = F(\alpha)$, where α is a root of $X^2 + 1 = 0$. The mapping $x + y\alpha \mapsto (x, y)$ induces a projection π of K^n onto F^{2n}; if $\mathbf{v} = \mathbf{x} + \mathbf{y}\alpha$, where $\mathbf{x}, \mathbf{y} \in F^n$, then $\pi(\mathbf{v}) = (x_1, y_1, ..., x_n, y_n)$.

Let $\psi: x + y\alpha \mapsto x - y\alpha$ denote the unique nontrivial automorphism of K as well as the componentwise extension of ψ which maps K^n onto K^n. Let $\beta = -1 - \alpha$, a primitive root of K.

Let Q be the set of nonzero squares in K, and $N = K^* - Q$; we observe that $Q = \{1, -1, \alpha, -\alpha\}$ and $N = \{1 + \alpha, 1 - \alpha, -1 + \alpha, -1 - \alpha\}$. For $\mathbf{v} = (v_i) \in K^n$, let $q(\mathbf{v}) = \#\{v_i : v_i \in Q\}$ and $n(\mathbf{v}) = \#\{v_i : v_i \in N\}$. Then the Hamming weight of πv is given by

$$\begin{aligned} wt(\pi\mathbf{v}) &= q(\mathbf{v}) + 2n(\mathbf{v}) \\ &= wt(\mathbf{v}) + n(\mathbf{v}). \end{aligned} \tag{*}$$

THEOREM. *Let* $\mathscr{C}$ *be the* $[6, 3]$ *code over* K *generated by*

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & \beta & \beta \\ 0 & 1 & 0 & \beta & 1 & \beta \\ 0 & 0 & 1 & \beta & \beta & 1 \end{pmatrix}.$$

Then (a) $\mathscr{C}$ *is a* $[6, 3, 4]$ *code over* K.

(b) $\mathscr{C}^{\perp} = \psi\mathscr{C}$,

(c) $\mathscr{C} \cap \psi\mathscr{C} = \{0\}$; *so* $\mathscr{C} \oplus \psi\mathscr{C} = K^6$.

(d) *The codes* $\pi\mathscr{C}$ *and* $\pi(\psi\mathscr{C})$ *are equivalent to the ternary Golay code* $\mathscr{G}_{12}$.

Proof. (a) Denote the rows of G by $\mathbf{r}_1$, $\mathbf{r}_2$, and $\mathbf{r}_3$. An easy check shows that for each $x \in K$, $wt(\mathbf{r}_1 + x\mathbf{r}_2) \geq 4$; it follows from the symmetry of G that any linear combination of two rows of G has weight at least 4. The right-half submatrix of G is nonsingular; therefore any linear combination of the three rows with nonzero coefficients has at least one nonzero component in its right half and so has weight at least 4.

(b) It suffices to show $\psi(\mathbf{r}_1) \in \mathscr{C}^{\perp}$; by symmetry, we need only to show $\psi(\mathbf{r}_1) \cdot \mathbf{r}_1 = \psi(\mathbf{r}_1) \cdot \mathbf{r}_2 = 0$. In fact, we have

$$\psi(\mathbf{r}_1) \cdot \mathbf{r}_1 = 2 + 2\beta^4 = 2 + 2 \cdot 2 = 0$$

$$\psi(\mathbf{r}_1) \cdot \mathbf{r}_2 = \beta + \beta^3 + \beta^4 = \beta + (1 - \beta) + 2 = 0.$$

(c) If $\mathbf{v} = v_1\mathbf{r}_1 + v_2\mathbf{r}_2 + v_3\mathbf{r}_3 \in \mathscr{C} \cap \psi\mathscr{C} = \mathscr{C} \cap \mathscr{C}^{\perp}$, then $0 = \mathbf{v} \cdot \mathbf{r}_i = (v_1 + v_2 + v_3) + (1 + \alpha) v_i$; it follows that each $v_i = 0$. Thus K^6 decomposes into the orthogonal spaces $\mathscr{C}$ and $\psi\mathscr{C}$.

(d) We note that for $x \in Q$, $x \cdot \psi x = 1$ and for $x \in N$, $x \cdot \psi x = 2$. Thus $\mathbf{v} \cdot \psi\mathbf{v} = q(\mathbf{v}) + 2n(\mathbf{v})$, where the sum on the right is interpreted modulo 3. But (c) and Eqs. (*), then, imply that for $\mathbf{v} \in \mathscr{C}$, $wt(\mathbf{v}) \equiv 0 \pmod 3$. Since $wt(\pi\mathbf{r}_i) = 6$, the minimum weight in $\pi\mathscr{C}$ is 6. So by the result of Pless, $\pi\mathscr{C}$ is equivalent to $\mathscr{G}_{12}$. The map $\pi \circ \psi \circ \pi^{-1}$ is an F-monomial equivalence of $\pi\mathscr{C}$ and $\pi\mathscr{C}^{\perp}$.

A second proof of part (d) relies on the observation that $(\pi\mathbf{v}) \cdot (\pi\mathbf{v}) = \mathbf{v} \cdot \psi v$. Part (c) then implies that each element of $\pi\mathscr{C}$ is isotropic. It follows that $\pi\mathscr{C}$ is self-orthogonal and that each weight is a multiple of 3.

As a final note, we reconstruct the Hamming weight enumerator of $\mathscr{G}_{12}$ by analyzing the Q-weight enumerator of $\mathscr{C}$. (See [4] for definitions and notation.) By Eqs. (*), we have $W^H_{\mathscr{G}_{12}}(1, x) = W^Q_{\mathscr{C}}(1, x, x^2)$. To obtain $W^Q_{\mathscr{C}}$, we note that the [6, 3, 4] code $\mathscr{C}$ is maximum distance separable [6], which determines its Hamming weight enumerator $W^H_{\mathscr{C}}(1, x) = 1 + 120x^4 + 240x^5 + 368x^6$. Because $q(\mathbf{v}) + 2n(\mathbf{v})$ is divisible by 3 for each $v \in \mathscr{C}$, the 120 weight-4 codewords have $q(\mathbf{v}) = n(\mathbf{v}) = 2$. The 240 weight-5 codewords split into equal sets with $q(\mathbf{v}) = 1$ and $q(\mathbf{v}) = 4$. (The map $\mathbf{v} \mapsto \beta\mathbf{v}$ provides the correspondence.) An enumeration establishes that 24 of the weight-6 codewords have $q(\mathbf{v}) = 6$; so another 24 have $q(\mathbf{v}) = 0$ and the remaining 320 have $q(\mathbf{v}) = 3$. Thus

$$W^Q_{\mathscr{C}}(1, x, y) = 1 + 120(xy^4 + x^2y^2 + x^4y) + 24(x^6 + y^6) + 320x^3y^3$$

and we recover the weight enumerator of $\mathscr{G}_{12}$ as

$$W^H_{\mathscr{G}_{12}}(1, x) = W^Q_{\mathscr{C}}(1, x, x^2) = 1 + 264x^6 + 440x^9 + 24x^{12}.$$

REFERENCES

1. P. J. CAMERON AND J. H. VAN LINT, "Graphs, Codes, and Designs," Cambridge Univ. Press, London/New York, 1980.
2. CONWAY, Three lectures on exceptional groups, *in* "Finite Simple Groups" (M. B. Powell and G. Higman, Eds.), Academic Press, New York, 1971.
3. M. GOLAY, Notes on digital coding, *Proc. IEE-E* **37** (1949), 657.
4. D. Y. GOLDBERG, A generalized weight for linear codes and a Witt-MacWilliams theorem, *J. Combin. Theeory Ser. A* **29** (1980), 363–367.
5. J. LEECH AND N. J. A. SLOANE, Sphere packings and error-correcting codes, *Canad. J. Math.* **23** (1971), 718–745.

6. F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes" North-Holland, Amsterdam, 1978.
7. V. Pless, On the uniqueness of the Golay codes, *J. Combin. Theory* **5** (1968), 215–228.
8. J. Wolfmann, A new construction of the binary Golay code (24, 12, 8) using a group algebra over a finite field, *Discrete Math.* **31** (1980), 337–338.